REMARKS

This communication is responsive to the Office Action dated 1 February 2007.

Prior to this paper, claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-44 and 46-54 were pending. In this paper, the Applicant has:

- amended claims 21, 25, 41, 47, 48, 51 and 52;
- cancelled claims 37 and 39; and
- added new claims 55 and 56.

The amendments to claims 21, 25, 41, 47, 48, 51 and 52 and new claims 55 and 56 are submitted to be completely supported by the application as originally filed and to add no new matter.

Claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44 and 46-56 are now pending.

A Request for Continued Examination is filed together herewith.

Claims 1, 3, 17, 25, 34-36, 38, 41, 42 and 47-50

The Examiner has raised the combination of US patent No. 6,052,780 (Glover) and US patent No. 6,892,306 (En-Seung et al.) in connection with claims 1, 3, 17, 25, 34-36, 38, 41, 42 and 47-50. The Applicant respectfully submits that claims 1, 3, 17, 25, 34-36, 38, 41, 42 and 47-50 patentably distinguish the combination of Glover and En-Seung et al.

As correctly identified by the Examiner on page 3 of the Office Action, Glover does not disclose the claim 1 feature of "receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key."

En-Seung et al. fail to remedy this deficiency.

As understood by the Applicant, En-Seung et al. disclose a digital cryptograph and encryption process which encrypts and transmits digital information (e.g. media content) requested by users. The En-Seung et al. system uses "key information", a "user's key" and a "temporary validation key" to decrypt and replay the encrypted digital information at the user's terminal. Each registered subscribing user is provided with unique key information which has a one-to-one correspondence with a number of identity characters particular to the registered subscribing user. The En-Seung et al. system generates the user's key by applying a key generation algorithm to the key information. A temporary validation key (created when the registered user accesses the server) is encrypted with the user's key. The digital content is encrypted using the temporary validation key in an encryption algorithm. The decryption algorithm allows the user to decrypt the temporary validation key using the user's key and then to decrypt the media content using the temporary validation key so as to replay the media content.

The Examiner appears to express the view, on page 3 of the Office Action, that the En-Seung et al. "temporary validation key" exhibits the characteristics of the claim 1 "decryption key" and that the En-Seung et al. "user's key" exhibits the characteristics of the claim 1 "user key". With respect, the Applicant submits that this view is incorrect. Claim 1 specifically recites "the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device". En-Seung et al. fail to teach or suggest this claim 1 feature. In direct contrast to this claim 1 feature, En-Seung et al. disclose that the "user's key" is based on user "identity characters" that are particular to the user (e.g. driver's license number, social security number etc.) and not to the user's computing device.

More specifically, En-seung et al. diclose:

(i) "the user's key is generated by using the key information" - (col. 5, ln. 19-20; col. 7, ln. 12-13);

(ii) the "key information" is generated on the basis of the "identity characters of the user" - (col. 7, ln. 6-7); and

(iii) "identity characters of the user" are disclosed as including "the user's social security number, the user's driver license number or the user's resident registration number" or a set of characters that "uniquely identify the user in the manner of the driver's license number" - (col. 7, ln. 28-31).

This aspect of En-Seung et al. clearly describes how the En-Seung et al. user's key is based on characteristics of the user and not the "user computing device" as recited in claim 1. En-Seung et al. explicitly teach away from the claim 1 feature that the "user key is bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device".

The Applicant submits further that it would not be obvious to modify the En-Seung et al. system to base its "user's key" on characteristics of the user computing device, because this represents a significant paradigm shift for the En-Seung et al. system. In the En-Seung et al. system, a user can obtain their user's key and access the encrypted digital information from different terminal units (10) provided that they have their "identity characters". In the Applicant's system, the user key is provided to a particular user computing device (as opposed to a particular user) and the user themselves is unaware of the characteristics used to bond the user key to the user computing device. Advantageously, the Applicant's system, as recited in claim 1, prevents fraudulent or otherwise unscrupulous use of "identity characters" by multiple users.

Moreover, En-Seung et al. specifically state that it is an object of the En-Seung et al. technology "to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using key information, a user's key, and a temporary validation key, and to decrypt and play the digital information at the terminal of the user by using the key information and user authorization information" - (col. 2, ln. 29-35). En-Seung et al. also state that these and other objects are obtained with an encryption and decryption process and apparatus wherein "the user must register membership information that includes the user's identity characters, with the server that controls the transmission of the digital information" - (col. 2, ln. 63 - col. 3, ln. 2). These statements from En-Seung et al. describe how it was an object of the En-Seung et al. system to have a user's

key that is based on the "identity characters" of the user and not on characteristics of the user's computer.

Based on these statements from En-Seung et al. together with the reasoning presented above, the Application submits that it would not be obvious to modify the En-Seung et al. system to base its "user's key" on characteristics of the user computing device.

Based on all of the arguments presented above, the Applicant submits that claim 1 patentably distinguishes the combination of Glover and En-Seung et al. Claims 3, 17, 25, 34-36, 38, 41, 42 and 47-50 depend from claim 1 and are submitted to patentably distinguish the combination of Glover and En-Seung et al. for at least this reason.

Additional Comments Relating to Claim 47

Claim 47 depends from claim 1 and is therefore submitted to be patentable for the reasons outline above. In addition, claim 47 (as amended) recites "receiving the file from a remote computer over a communication network that includes the remote server from which the decryption key is obtained but through a communication path that does not include the remote server from which the decryption key is received". Neither Glover nor En-Seung et al. teach or suggest this claim 47 feature.

Claim 47 recites that the file (e.g containing encrypted media content) is received from a "remote computer" through a network that includes the"remote server" from which the decryption key is received, but over a communication path that does not include the remote server from which the decryption key is received - i.e. that the encrypted media and the decryption key are received from different computers. Glover teaches that encrypted media content may be purchased separately (e.g. on a DVD) and that the "decryption key" may then be received from the "content provider" when the user calls a toll-free telephone number - (col. 21, ln. 20-65). This aspect of Glover does not amount to receiving a media file and a decryption key over a single communication network from two different computers as recited in claim 47. Glover also teaches an "on-line" embodiment where the media content and the "decryption key" are both downloaded from a "service provider" - (col. 22, ln. 1-20). Glover

specifically discloses that the decryption "algorithms are downloaded at the time of recording from a service provider" (col. 22, ln. 12-13) and that the encrypted media content is provided to the service provider "to present to their customers" (col. 22, ln. 14-15). In the Glover "on-line" embodiment, the "service provider" provides end users with both the encrypted content and the decryption algorithms. Accordingly, Glover fails to teach or suggest that the media content and the decryption key are received over a single communication network from two different computers as recited in claim 47.

On page 7 of the Office Action, the Examiner contends that Figures 3 and 4 of En-Seung et al. disclose the claim 47 feature of receiving the file and the decryption key over a single communication network but from different computers. With respect, the Applicant submits that this contention is erroneous. Figures 3 and 4 of En-Seung et al. clearly show (e.g. by way of non-enumerated arrows) that the only component in communication with the user "terminal unit" 20 (claim 47) is "service server" 22. Figures 3 and 4 of En-Seung et al. are described at col. 7, ln. 32-67. This passage from En-Seung et al. states that "[s]ervice server 22 generates a temporary validation key" - (col. 7, ln. 52-54). This En-Seung et al. "temporary validation key" is alleged by the Examiner to have the characteristics of the claim 1 "decryption key" - (page 3 of the Office Action). En-Seung et al. also states that "[s]ervice server 22 adds the digital information ... to form the copyright protection protocol and then transmits the copyright protection protocol to terminal unit 20" - (col. 7, ln. 56-61). The "digital information" referred to by En-Seung et al. is media content. Accordingly, En-Seung et al. specifically teach that both the decryption key and the media content are received from the same "service server" 22. This contrasts directly, with the claim 47 feature of receiving the file and the decryption key over a single communication network from different computers. Moreover, host server 23 shown in Figures 3 and 4 of En-Seung et al. is only disclosed as generating "key information" and transmitting this "key information" to service server 22 - (col. 7, ln. 62-67). Host server 23 is not disclosed as transmitting any information to the user computing device (terminal unit 20).

Figures 3 and 4 of En-Seung et al. clearly show that all components of the En-Seung et al. system communicate with terminal unit 20 through service server 22. En-Seung et al.

clearly states that "[s]ervice server 22 generates a temporary validation key" - (col. 7, ln. 52-54). This En-Seung et al. "temporary validation key" is alleged by the Examiner to have the characteristics of the claim 1 "decryption key" - see page 3 of the Office Action. Accordingly, En-Seung et al. explicitly disclose that the communication path through which encrypted files are received at terminal unit 20 includes service server 22 (i.e. the same server which sends the decryption key). In direct contrast, claim 47 (as amended) recites that the file is received through a communication path that does not include the server from which the decryption key is received.

Based on this reasoning, the Applicant submits that claim 47 further patentably distinguishes the combination of Glover and En-Seung et al.

Additional Comments Relating to Claims 48-50

Claim 48 depends from claim 1 and is therefore submitted to be patentable for the reasons outline above. In addition, claim 48 recites the combination of "sending the file from the user computing device to a second user computing device over a communication network; upon receipt of the file at the second user computing device: sending a request, from the second user computing device to the remote server, for the decryption key; receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and responding to receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral decryption engine and the decryption key". Neither Glover nor En-Seung et al. teach or suggest this claim 48 combination of features.

More particularly, neither Glover nor En-Seung et al. disclose or suggest "sending the file from the user computing device to a second user computing device over a communication network" and then repeating the decryption process at the second user computing device as recited in claim 48. As discussed above in relation to claim 47, Glover describes a first

embodiment where a user separately obtains a DVD and then communicates with the "content provider" via telephone to obtain encryption information to decrypt the media content contained on the DVD and a second embodiment where a user corresponds with the "service provider" to obtain both the media content and the encryption information. Glover does not teach or disclose that encrypted media files are sent between users and that each user then accesses decryption information from the same centralized "remote server". Accordingly, Glover fails to disclose the claim 48 feature of "sending the file from the user computing device to a second user computing device over a communication network" and then repeating the decryption process at the second user computing device.

The Examiner expresses the view that En-Seung et al. disclose the features of claim 48 at col. 6, ln. 30-36 and col. 7, ln. 6-16 and 52-61. The Applicant respectfully submits that this view is incorrect. None of these passages from En-Seung et al. disclose or suggest that media files are transferred between user computing devices. Neither these passages nor any other part of En-Seung et al. teach the claim 48 combination "sending the file from the user computing device to a second user computing device over a communication network" and then repeating the decryption process at the second user computing device. As discussed above in relation to claim 47, En-Seung et al. specifically disclose that both the media content and the decryption information are downloaded from "service server" 22 (in the embodiment of Figures 3 and 4) or from "service server" 12 (in the embodiment of Figures 1 and 2).

In addition to the above-described differences, claim 48 recites, after receiving the file at the second user computing device, "receiving the decryption key from the remote server at the second user computing device ... and decrypting the media content at the second user computing device using the integral decryption engine and the decryption key". The use of the definite article "the" to describe "the decryption key" in claim 48 implies that the decryption key received at the second user computing device is the same as the decryption key received at the first user computing device. The En-Seung et al. system does not support the use of one "decryption key" that can be used by multiple users on different computers at the same or different times. The Examiner alleges that the "decryption key" recited in claims 1 and 48 is akin to the En-Seung et al. "temporary validation key" - see page 3 of the Office Action. En-

Seung et al. specifically teach that the temporary validation key remains "valid only while the user is in the process of accessing the system, that is temporarily" (col. 5, ln. 40-42) and that temporary validation keys are different depending on the time that a user accesses the system (col. 5, ln. 38-40). This aspect of En-Seung et al. teaches directly away from the claim 48 feature of using the same decryption key at two different user computing devices.

Based on this reasoning, the Applicant submits that claim 48 further patentably distinguishes the combination of Glover and En-Seung et al. Claims 49 and 50 depend from claim 48 and are submitted to further distinguish the combination of Glover and En-Seung et al. for the same reasons.

Additional Comments Relating to Claims 25 and 41

Claims 25 and 41 depend from claim 1 and are therefore submitted to be patentable for the reasons outline above. In addition, claims 25 and 41 (as amended) recite "receiving the file at the user computing device comprises downloading the file using a peer to peer network from a remote computer that is different from the remote server". Neither Glover nor En-Seung et al. teach or suggest this feature.

As discussed above, Glover discloses obtaining the "file" (e.g. media content) in the form of a DVD and then obtaining decryption information from the "content provider" over the telephone. Glover also discloses an "on-line" embodiment where both the media content and decryption algorithms are downloaded from a "service provider". As discussed above in relation to claim 47, neither of these embodiments disclosed by Glover et al. involve downloading media content and decryption information from different computers. Moreover, the "content provider" and "service provider" disclosed by Glover et al. are not "peers" in the sense of a "peer to peer network" as recited in claims 25 and 41. A "peer to peer network" involves a network of similar users (peers) and not a server/client model as described by Glover.

Similarly, as discussed above, En-Seung et al. teach that both decryption information and media content are downloaded to terminal unit 20 through service server 22. Accordingly,

En-Seung et al. fail to disclose downloading media content and decryption information from different computers. Moreover, the "service server" 22 of the En-Seung et al. system is a server that forms part of a server/client network architecture. The En-Seung et al. service server 22 is not a "peer" in the sense of a "peer to peer network" as recited in claims 25 and 41. A "peer to peer network" involves a network of similar users (peers) and not the server/client architecture taught by En-Seung et al.

Based on this reasoning, the Applicant submits that claims 25 and 41 further patentably distinguish the combination of Glover and En-Seung et al.

Claims 2, 18 and 20

The Examiner has raised the combination of Glover, En-Seung et al. and US patent No. 6,564,248 (Budge et al.) in connection with claims 2, 18 and 20. Claims 2, 18 and 20 depend from claim 1. As discussed above, claim 1 patentably distinguishes the combination of Glover and En-Seung et al. The Applicant respectfully submits that Budge et al. fails to remedy the aforementioned shortcomings of Glover and En-Seung et al. and, consequently, claims 2, 18 and 20 patentably distinguish the combination of Glover, En-Seung et al. and Budge et al.

Claims 27 and 40

The Examiner has raised the combination of Glover, En-Seung et al. and US patent No. 6,385,596 (Wiser et al.) in connection with claims 27 and 40. Claims 27 and 40 depend from claim 1. As discussed above, claim 1 patentably distinguishes the combination of Glover and En-Seung et al. The Applicant respectfully submits that Wiser et al. fails to remedy the aforementioned shortcomings of Glover and En-Seung et al. and, consequently, claims 27 and 40 patentably distinguish the combination of Glover, En-Seung et al. and Wiser et al.

Claims 4-6, 11, 28, 31, 43, 44 and 51-54

The Examiner has raised the combination of Glover, Budge and En-Seung et al. in connection with claims 4-6, 11, 28, 31, 43, 44 and 51-54. The Applicant respectfully submits that claims 4-6, 11, 28, 31, 43, 44 and 51-54 patentably distinguish the combination of Glover, Budge and En-Seung et al.

As correctly identified by the Examiner on page 10 of the Office Action, neither Glover nor Budge et al. disclose the claim 4 feature of "obtain a decryption key from a remote server, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key".

The Applicant submits that En-Seung et al. fail to remedy this deficiency.

The Examiner appears to express the view, on page 10 of the Office Action, that the En-Seung et al. "temporary validation key" exhibits the characteristics of the claim 4 "decryption key" and that the En-Seung et al. "user's key" exhibits the characteristics of the claim 4 "user key". The Applicant respectfully submits that this view is incorrect. Claim 4 specifically recites "the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key". As discussed above, En-Seung et al. fail to teach or suggest this claim 4 feature. In direct contrast to this claim 4 feature, En-Seung et al. disclose that the "user's key" is based on user "identity characters" that are particular to the user (e.g. driver's license number, social security number etc.) and not to the user's computing device.

Based on this reasoning, the Applicant submits that claim 4 patentably distinguishes the combination of Glover, Budge et al. and En-Seung et al. Claims 5, 6, 11, 28, 31, 43, 44 and 51-54 depend from claim 4 and are submitted to patentably distinguish the combination of Glover, Budge et al. and En-Seung et al. for at least this reason.

Additional Comments Relating to Claim 51

Claim 51 depends from claim 4 and is therefore submitted to be patentable for the reasons outline above. In addition, claim 51 (as amended) recites "wherein the communication network from which the single file is downloaded includes the remote server from which the decryption key is obtained and wherein downloading the single file from the computer via the

communication network comprises downloading the single file from the computer through a communication path that does not include the remote server from which the decryption key is obtained". The combination of Glover, En-Seung et al. and Budge et al. fail to teach or suggest this claim 51 feature.

Like claim 47 discussed above, claim 51 recites that the single file (containing encrypted media content) is received from a "computer" that is part of the same communication network but is different from the "remote server" from which the decryption key is received - i.e. that the encrypted media and the decryption key are received from different computers. As discussed above in relation to claim 47, both Glover and En-Seung et al. disclose obtaining media content and decryption keys from the same source. Neither Glover nor En-Seung et al. suggest that the media content and the decryption key are received from different computers as recited in claim 51.

Furthermore, claim 51 (as amended) recites that the single file is downloaded "through a communication path that does not include the remote server from which the decryption key is obtained". As discussed above in relation to claim 47, neither Glover nor En-Seung et al. disclose this feature.

Budge et al. fail to remedy these deficiencies.

Based on this reasoning, the Applicant submits that claim 51 further patentably distinguishes the combination of Glover, Budge et al. and En-Seung et al.

Additional Comments Relating to Claims 52-54

Claim 52 depends from claim 4 and is therefore submitted to be patentable for the reasons outline above. In addition, claim 52 recites the combination of "sending the file from the user computing device to a second user computing device over a communication network; upon receipt of the file at the second user computing device: sending a request, from the second user computing device to the remote server, for the decryption key; receiving the decryption key from the remote server at the second user computing device, the decryption key

itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and responding to receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral decryption engine and the decryption key". The combination of Glover, En-Seung et al. and Budge et al. fail to teach or suggest this claim 52 combination of features.

More particularly, as discussed above in relation to claim 48, neither Glover nor En-Seung et al. disclose or suggest "sending the file from the user computing device to a second user computing device over a communication network" and then repeating the decryption process at the second user computing device.

In addition, claim 52 recites "receiving the decryption key from the remote server at the second user computing device ... decrypting the media content at the second user computing device using the integral decryption engine and the decryption key". The use of the definite article "the" to describe "the decryption key" in claim 52 implies that the decryption key received and used at the second user computing device is the same as the decryption key received and used at the first user computing device. As discussed above in relation to claim 48, neither Glover nor En-Seung et al. support the use of one "decryption key" that can be used by multiple users at different user computing devices at the same or different times.

Budge et al. fails to remedy these deficiencies.

Based on this reasoning, the Applicant submits that claim 52 further patentably distinguishes the combination of Glover, En-Seung et al. and Budge et al. Claims 53 and 54 depend from claim 52 and are submitted to further distinguish the combination of Glover, En-Seung et al. and Budge et al. for the same reasons.

Claim 33

The Examiner has raised the combination of Glover, En-Seung et al., Budge et al. and Wiser et al. in connection with claim 33. Claim 33 depends from claim 4. As discussed above, claim 4 patentably distinguishes the combination of Glover, En-Seung et al. and Budge et al. The Applicant respectfully submits that Wiser et al. fails to remedy the aforementioned shortcomings of Glover, En-Seung et al. and Budge et al. and, consequently, claim 33 patentably distinguishes the combination of Glover, En-Seung et al., Budge et al. and Wiser et al.

Claim 21

The Applicant has amended claim 21 to depend from claim 4. As discussed above, claim 4 patentably distinguishes the prior art of record. The Applicant submits that claim 21 (as amended) patentably distinguishes the prior art of record for at least this reason.

Claims 55 and 56

The Applicant has added new claims 55 and 56 for which patent protection is sought. Claims 55 and 56 are completely supported by the application as originally filed and add no new matter. The Applicant submits that claims 55 and 56 patentably distinguish the prior art of record.

Conclusions

In view of the foregoing amendments and arguments, the Applicant respectfully submits that this application is now in condition for allowance and requests reconsideration and allowance of this application.

Respectfully submitted,
OYEN WIGGS GREEN & MUTALA

By: 

Richard A. Johnson
Vancouver, Canada
tel: 604.669.3432
fax: 604.681.4081
e-mail: RAJDocket@patentable.com